UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,239	01/26/2001	Jeffrey Bruce Lotspiech	ARC920010006US1	6974

7590 11/24/2004

John L. Rogitz
Rogitz & Associates
Suite 3120
750 B Street
San Diego, CA 92101

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 11/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/771,239	LOTSPIECH ET AL.	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20040904*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received 21 September 2004. Claims 3, 13, and 22 have been amended. Claim 2 has been canceled. No claims have been added. Claims 1 and 3-30 are pending in the present application.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 20 September 2004 was filed after the mailing date of the first Office action on 17 August 2004. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Amendment

3. The declaration filed on 21 September 2004 under 37 CFR 1.131 has been considered but is ineffective to overcome the Yoshida reference.

Specifically, the declaration has not been signed by all of the inventors. See MPEP § 715.04 I. (A). Further, the declaration does not comply with any of the requirements of MPEP § 715.04 I. (B)-(D). Although Applicant states that the inventor Lotspiech is on retirement leave and is unavailable until January, this is not sufficient to meet the requirement that it is "not possible to produce the affidavit or declaration of the

inventor", nor does it sufficiently show that "a joint inventor is deceased, refuses to sign, or is otherwise unavailable". Specifically, the previous Office action was mailed on 17 August 2004. The Examiner wishes to remind Applicant that by filing a Petition for Extension of Time, as per 37 CFR 1.136(a), Applicant would have been able to file a timely response to the previous Office action on or before 17 February 2005. This would have allowed sufficient time for inventor Lotspiech to review and sign the declaration upon his return in January.

It is noted that, were the declaration signed by all of the inventors, it would be effective to show conception of all of the claimed subject matter with the following exceptions. The exhibit accompanying the declaration does not explicitly disclose "determining whether the traitor subset represents at least two traitor receivers" as recited in Claims 1, 13, and 22, although the exhibit does appear to support determining whether the traitor subset represents at least two traitor receiver candidates as in Applicant's disclosure (Figure 15 and page 17). The exhibit also does not explicitly disclose "subsets $S_{i1},\ldots,S_{im}$ having associated subset keys $L_{i1},\ldots,L_{im}$" or "encrypting the session key K and the false key with the subset keys" as recited in Claims 8, 18, and 28, although there is support for the subsets $S_{i1},\ldots,S_{im}$ themselves, and for encoding with the partition consisting of those subsets. It is also not clear how the exhibit shows conception of the limitations of Claims 9-11, 19, and corresponding limitations in claim 28.

Response to Arguments

4. Applicant's arguments filed 21 September 2004 have been fully considered but they are not persuasive.

Regarding the rejections of Claims 1 and 3 under 35 U.S.C. 102(e) as being anticipated by Schwenk, US Patent 6222923, Applicant asserts that Schwenk teaches neither dividing a subset nor removing a complementary subset, and that Schwenk only teaches finding the intersection of two subsets. The Examiner respectfully disagrees. On the contrary, the intersection operation necessarily divides and removes. By finding the intersection of two sets that are each known to contain a traitor receiver, the subset that is the result of the intersection, which therefore must contain the traitor receiver, is divided from its complementary subset, which consists of the members of the two original sets that are not elements of the intersection. Therefore, the Examiner maintains the rejection set forth below.

Regarding the rejections of Claims 4-30 under 35 U.S.C. 103(a) as being unpatentable over Schwenk in view of Yoshida et al, "A Subscriber-Excluding and Traitor-Tracing Broadcast Distribution System", Applicant attempts to antedate the Yoshida reference and further argues that there is no fair suggestion to combine the references. Applicant further argues that Yoshida does not teach encoding with a false key. Applicant's filing of a declaration under 37 CFR 1.131 attempting to antedate the Yoshida reference has been addressed above.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, firstly, the Examiner believes that the cited motivation for combining the references, to increase the efficiency of a traitor-tracing system, is germane to both Yoshida and Schwenk, as both discuss systems for identifying and disabling traitor receivers. Further, Applicant states that Schwenk "does nothing to find traitors other than determining device subset intersections without ever evidently drilling down into the subsets". However, the Examiner draws Applicant's attention to the fact that Schwenk discloses that the central location, once it has determined the identity of a traitor, can block the traitor from using the system (column 4, lines 29-35). Schwenk further states that the use of such a small key hierarchy was for illustrative purposes and was not a limit on the size of hierarchy that can be used (column 4, lines 35-39); Applicant's argument appears to be based on the assumption that the example used was to be taken as a limit of the system. The Examiner therefore believes that a suggestion to combine the references was reasonable, as both are generally directed to finding and disabling traitors in a broadcast system. Although Applicant states that the techniques used by Schwenk and Yoshida differ, the Examiner believes that there is nothing in either reference that would

explicitly contradict such a combination, and that therefore the cited motivation above is a reasonable suggestion to combine the methods of Schwenk and Yoshida.

In response to Applicant's argument that Yoshida does not teach encoding with a false key, the Examiner wishes to clarify the rejection of the previous Office action. Yoshida discloses the special value that indicates that a subscriber is an excluded subscriber. The special value is output instead of a session key when the subscriber is in fact excluded (see page 249, column 2, lines 15-26). Therefore, because the special value is output where a session key would normally be expected, the Examiner believes that the special value reads on "false key". Further, Yoshida discloses that, in order to determine the set of traitor receivers, an enabling part is generated by using an encryption algorithm that takes the session key as one of its inputs (see page 251, column 1, lines 4-15). The Examiner therefore believes that the subsets are thus encoded with a false key. For the above reasons, the Examiner maintains the rejection set forth below.

Specification

5. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claims 1, 13, and 22, as amended, recite the limitation "determining whether the traitor subset represents at least two traitor receivers, and if so, dividing the traitor subset into two child sets". There is no support in the

specification for performing such a division based on the determination of whether a subset represents at least two traitor receivers. This is described in further detail below in reference to the rejection under 35 U.S.C. 112, first paragraph.

Claim Rejections - 35 USC § 112

6. The rejection of Claims 3, 13, 14, 22, and 23 under 35 U.S.C. 112, second paragraph, as being indefinite is withdrawn in light of the amendments to the claims. The rejection of Claim 2 is rendered moot in view of the cancellation of the claim, and is therefore also withdrawn.

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 1, 3-11, 13-14, 22-23, and 29-30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically, Claims 1, 13, and 22, as amended, recite the limitation "determining whether the traitor subset represents at least two traitor receivers, and if so, dividing the traitor subset into two child sets". There is no support in Applicant's disclosure for performing such a division

based on the determination of whether a subset represents at least two traitor receivers. Applicant cites blocks 108 and 112 of Figure 15 as support for the amendments to the claims. The Examiner notes that both in Figure 15 and at page 17, line 15-page 18, line 2 of Applicant's specification, there is support for determining whether the traitor subset contains at least two traitor receiver candidates and dividing the traitor subset based on that determination. It is assumed that it is this latter interpretation which is intended in the claims. Claims 3-11, 14, 23 and 29-30 are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1 and 3 are rejected under 35 U.S.C. 102(e) as being anticipated by Schwenk, US Patent 6222923.

In reference to Claims 1 and 3, Schwenk discloses a method including receiving a set of subsets derived from a tree including leaves, each of which represents a receiver (column 3, lines 24-33); identifying a traitor subset as containing at least one

traitor receiver (column 4, lines 9-13); and identifying and disabling the traitor receiver (column 4, lines 33-36). Schwenk further discloses dividing the traitor subset into child subsets and removing complementary subsets (column 4, lines 8-33).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 4-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwenk in view of Yoshida et al, "A Subscriber-Excluding and Traitor-Tracing Broadcast Distribution System".

In reference to Claims 4, 29, and 30, Schwenk discloses everything as applied to Claim 1 above. However, Schwenk does not explicitly disclose encoding subsets with a false key. Schwenk also does not disclose traitor receivers embodied in a clone.

Yoshida discloses a method and system for excluding and tracing traitor subscribers to a broadcast distribution system. In reference to Claims 4 and 30, Yoshida discloses that the method includes encoding subsets with a false key (the special value of page 249, column 2, lines 15-26). In reference to Claim 29, Yoshida discloses using a captured or cloned pirate decoder to identify a traitor (page 249, column 2, lines 32-37).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schwenk to include encoding subsets with a false key and to further include the use of a clone, in order to increase the efficiency of the system with regard to the size of storage and bandwidth required (see Yoshida, page 248, column 1, lines 15-22).

In reference to Claims 5-7, Yoshida further discloses executing a binary search (page 254, column 1, lines 19-25).

In reference to Claim 8, Schwenk discloses everything as applied to Claim 1 above. Schwenk further discloses assigning each receiver private information (column 3, lines 42-51), selecting a session key (column 3, lines 55-62), partitioning receivers into subsets having subset keys (column 3, lines 36-42), and encrypting the session key with the subset keys (column 3, lines 55-58). However, Schwenk does not explicitly disclose encrypting the false key with the subset keys.

Yoshida discloses a method and system for tracing traitor subscribers in a broadcast distribution system that includes encrypting a false key (page 249, column 2, lines 15-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schwenk to include encrypting the false key with the subset key, in order to increase the efficiency of the system with regard to the size of storage and bandwidth required (see Yoshida, page 248, column 1, lines 15-22).

In reference to Claims 9 and 10, Schwenk further discloses that each receiver is assigned keys from nodes above the receiver in the tree (column 3, lines 42-58).

In reference to Claim 11, Schwenk further discloses initializing a spanning tree (column 4, lines 8-33).

In reference to Claim 12, Schwenk discloses a computer program device including a means for accessing a tree (column 3, lines 24-33), encrypting a session key (column 3, lines 55-58), identifying a traitor subset (column 4, lines 9-13), and using the traitor subset to identify and disable the traitor device (column 4, lines 33-36). However, Schwenk does not explicitly disclose encrypting a false key.

Yoshida discloses a method and system for tracing traitor subscribers in a broadcast distribution system that includes encrypting a false key (page 249, column 2, lines 15-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Schwenk to include encrypting the false key, in order to increase the efficiency of the system with regard to the size of storage and bandwidth required (see Yoshida, page 248, column 1, lines 15-22).

In reference to Claims 13 and 14, Schwenk further discloses dividing the traitor subset into child subsets and removing complementary subsets (column 4, lines 8-33).

In reference to Claims 15-17, Yoshida further discloses executing a binary search (page 254, column 1, lines 19-25).

In reference to Claim 18, Schwenk further discloses assigning each receiver private information (column 3, lines 42-51), selecting a session key (column 3, lines 55-62), partitioning receivers into subsets having subset keys (column 3, lines 36-42), and encrypting the session key with the subset keys (column 3, lines 55-58). Additionally, Yoshida further discloses encrypting a false key (page 249, column 2, lines 15-26).

In reference to Claim 19, Schwenk further discloses that each receiver is assigned keys from nodes above the receiver in the tree (column 3, lines 42-58).

In reference to Claim 20, Schwenk discloses a system for determining the identity of a traitor receiver and rendering it useless for decrypting data (column 4, lines 33-36). However, Schwenk does not explicitly disclose using a false key to encode subsets.

Yoshida discloses a method and system for tracing traitor subscribers in a broadcast distribution system that includes encoding subsets with a false key (page 249, column 2, lines 15-26). Yoshida further discloses using the captured pirate receiver for identifying and disabling the traitor receivers (page 249, column 2, lines 32-37).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Schwenk to include encoding subsets with a false key, in order to increase the efficiency of the system with regard to the size of storage and bandwidth required (see Yoshida, page 248, column 1, lines 15-22).

In reference to Claim 21, Schwenk further discloses receiving a set of subsets derived from a tree including leaves, each of which represents a receiver (column 3, lines 24-33); identifying a traitor subset as containing at least one traitor receiver (column 4, lines 9-13); and identifying the traitor receiver (column 4, lines 33-36).

In reference to Claims 22 and 23, Schwenk further discloses dividing the traitor subset into child subsets and removing complementary subsets (column 4, lines 8-33).

In reference to Claim 24, Yoshida further discloses encoding subsets with the false key (page 249, column 2, lines 15-26).

In reference to Claim 25-27, Yoshida further discloses executing a binary search (page 254, column 1, lines 19-25).

In reference to Claim 28, Schwenk further discloses assigning each receiver private information (column 3, lines 42-51), selecting a session key (column 3, lines 55-62), partitioning receivers into subsets having subset keys (column 3, lines 36-42), and encrypting the session key with the subset keys (column 3, lines 55-58). Schwenk additionally discloses that each receiver is assigned keys from nodes above the receiver in the tree (column 3, lines 42-58). Additionally, Yoshida further discloses encrypting a false key (page 249, column 2, lines 15-26).

Conclusion

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

Andrew Caldwell
Andrew Caldwell